encrypted digital content being decrypt-able according to a decryption key (KD) obtained from the license;

a content/package ID identifying one of the digital content and the package; and

license acquisition information including a location of a license provider for providing the license.

107. The package of claim 106 wherein the license acquisition information is in an unencrypted form.

108. The package of claim106 wherein the license provider location is a network address.

109. The package of claim 108 wherein the license provider location is an Internet address.

110. The package of claim 106 wherein the package is provided by a content provider having a public key and a private key, the package further including the content provider public key.

111. The package of claim 110 wherein the content provider public key is

encrypted according to the decryption key (KD).

112. The package of claim 111 wherein the encrypted content provider public key is signed by the content provider private key, and wherein alteration of the encrypted content provider public key prevents validation of the package.

113. The package of claim 110 wherein the content provider public key is signed by the content provider private key, wherein alteration of the content provider public key prevents validation of the package.

114. The package of claim 106 further comprising a key ID identifying the decryption key (KD).

115. The package of claim 106 wherein the package is provided by a content provider authorized by a root source to provide the package, the package further comprising a certificate from the root source indicating that the content provider has authority from the root source to provide the package.

116. The package of claim 115 wherein the content provider has a public key and a private key, and wherein the certificate includes the public key of the content provider.

117. The package of claim 116 wherein the root source has a public key and a private key, wherein the certificate is signed with the private key of the root source, and wherein the public key of the root source must be obtained to decrypt the encrypted signature.

118. The package of claim 106 wherein the package is provided by a content provider authorized by an intermediary source to provide the package, the intermediary source in turn being authorized by a root source to authorize the content provider, the package further comprising a first certificate from the root source indicating that the intermediary source has authority from the root source to authorize the content provider, and a second certificate from the intermediary source indicating that the content provider has authority from the intermediary source to provide the package.

119. The package of claim 118 wherein the content provider has a public key and a private key, wherein the intermediary source has a public key and a private key, wherein the first certificate includes the public key of the intermediary source, and wherein the second certificate includes the public key of the content provider.

120. The package of claim 119 wherein the root source has a public key and a private key, wherein the first certificate is signed with the private key of the root source, wherein the second certificate is signed with the private key of the intermediary source, wherein the public key of the root source must be obtained to decrypt the encrypted signature of the first

certificate, and wherein the public key of the intermediary source is obtained from the first certificate to decrypt the encrypted signature of the second certificate.

121. A computer-readable medium having stored thereon a data structure corresponding to a digital content package, the data structure including:

a first data field containing encrypted digital content to be rendered in accordance with a corresponding digital license, the data structure being separate and apart from the license, the encrypted digital content being decrypt-able according to a decryption key (KD) obtained from the license;

a second data field containing a content/package ID identifying one of the digital content and the package; and

a third data field containing license acquisition information including a location of a license provider for providing the license.

122. The data structure of claim 121 wherein the license acquisition information is in an unencrypted form.

123. The data structure of claim 121 wherein the license provider location is a network address.

124. The data structure of claim 123 wherein the license provider location is an

Internet address.

125. The data structure of claim 121 wherein the data structure is provided by a content provider having a public key and a private key, the data structure further including a fourth data field containing the content provider public key.

126. The data structure of claim 125 wherein the content provider public key is encrypted according to the decryption key (KD).

127. The data structure of claim 126 wherein the encrypted content provider public key is signed by the content provider private key, and wherein alteration of the encrypted content provider public key prevents validation of the data structure.

128. The data structure of claim 125 wherein the content provider public key is signed by the content provider private key, wherein alteration of the content provider public key prevents validation of the data structure.

129. The data structure of claim 121 further comprising a fourth data field containing a key ID identifying the decryption key (KD).

130. The data structure of claim 121 wherein the data structure is provided by a

content provider authorized by a root source to provide the data structure, the data structure further comprising a fourth data field containing a certificate from the root source indicating that the content provider has authority from the root source to provide the data structure.

131. The data structure of claim 130 wherein the content provider has a public key and a private key, and wherein the certificate includes the public key of the content provider.

132. The data structure of claim 131 wherein the root source has a public key and a private key, wherein the certificate is signed with the private key of the root source, and wherein the public key of the root source must be obtained to decrypt the encrypted signature.

133. The data structure of claim 121 wherein the data structure is provided by a content provider authorized by an intermediary source to provide the data structure, the intermediary source in turn being authorized by a root source to authorize the content provider, the data structure further comprising a fourth data field containing a first certificate from the root source indicating that the intermediary source has authority from the root source to authorize the content provider, and a fifth data field containing a second certificate from the intermediary source indicating that the content provider has authority from the intermediary source to provide the data structure.

134. The data structure of claim 133 wherein the content provider has a public

key and a private key, wherein the intermediary source has a public key and a private key, wherein the first certificate includes the public key of the intermediary source, and wherein the second certificate includes the public key of the content provider.

135. The data structure of claim 134 wherein the root source has a public key and a private key, wherein the first certificate is signed with the private key of the root source, wherein the second certificate is signed with the private key of the intermediary source, wherein the public key of the root source must be obtained to decrypt the encrypted signature of the first certificate, and wherein the public key of the intermediary source is obtained from the first certificate to decrypt the encrypted signature of the second certificate.

In the Abstract:

Please delete the Abstract and insert the following:

--A digital content package includes encrypted digital content to be rendered in accordance with a corresponding digital license and is separate and apart from the license. The encrypted digital content is decrypt-able according to a decryption key (KD) obtained from the license. The package also includes a content/package ID that identifies one of the digital content and the package, and license acquisition information including a location of a license provider for providing the license.--

Remarks